郴州技师学院文件

郴技〔2023〕50号

关于印发《郴州技师学院信息安全总体方针》《郴州技师学院个人信息管理制度》《郴州技师学院网络安全事件应急预案》的通知

院属各部门、单位:

现将《郴州技师学院信息安全总体方针》《郴州技师学院个人信息管理制度》《郴州技师学院网络安全事件应急预案》印发给你们，请遵照执行。

郴州技师学院

2023年11月27日

郴州技师学院信息安全总体方针

第一章 总则

第一条 为加强郴州技师学院（以下简称“我院”）信息技术管理与规范，完善单位内部管理结构，提高信息技术管理水平，特制定本管理办法。

第二条 信息系统安全管理是指我院在运用信息技术过程中，制定的有关信息系统安全决策权分配和责任承担的框架，主要包括在信息系统安全原则、信息系统安全架构、信息系统安全基础设施、信息系统安全应用和信息系统安全投入五个方面制定相关制度并建立有效工作机制，实现信息系统安全决策的责任和权力的有效分配与控制，提高信息系统安全资源的有效性、可用性和安全性。

第三条 信息系统安全管理是我院创建文明、平安校园的重要组成部分，我院通过建立有效的信息系统安全管理机制，持续巩固和提升信息系统安全能力，合理利用信息系统安全资源，有效管理信息系统安全风险。

第四条 本方案适用于我院所有与信息系统安全相关的所有活动。

第二章 组织机构与职责

第五条 根据成立网络与信息安全工作领导小组的通知，领导小组下设网络与信息安全办公室（设在后勤处）。学院领导、各系部处室主要负责人是落实网络与信息安全工作的第一

责任人。

第六条 学院网络与信息安全工作领导小组负责制定信息系统安全管理的办法和规定，协调和处理有关计算机信息系统安全的重大问题。

第七条 学院后勤处负责信息系统安全监督、安全事故调查；负责制定本单位信息系统安全管理制度、技术规范、控制措施等，并检查执行情况；负责对计算机病毒感染的预防、检测和清除；负责定期维护计算机软件和数据、对重要信息定期进行检查和备份；负责制定计算机信息系统安全管理办法的实施细则和技术规范，并督促执行。与相关处室协同组织对信息系统安全管理人员开展安全教育培训。

第八条 分管信息安全工作的负责人和信息安全技术管理人员，必须在接受专门的计算机信息安全培训后，方能从事计算机信息安全管理工作。

第三章 信息安全治理原则和目标

第九条 信息系统安全原则是指导单位有效运用信息系统安全来实现本单位服务目标的基本方针。根据单位相关管理规范，确定本单位信息系统安全原则如下:

1. 满足和推动业务发展;

2. 对新应用快速、稳定实现;

3. 信息系统安全架构完整、统一;

4. 数据集中、信息共享;

5. 控制成本、提高工作效率;

6.利用相关法律法规、国家标准规范本单位管理;

第十条 为有效开展信息系统安全管理工作，确保我院能够利用信息系统安全增强服务能力。根据我院建设规划，确定我院信息系统安全管理目标如下:

1.明确信息系统安全决策的权力和责任;

2.实现技术和业务的有效匹配;

3.实现信息系统安全资源的最优配置;

4.实现信息系统安全风险的可管可控。

第十一条 制定公开、可行的信息系统安全管理流程，建立业务与信息系统安全之间清晰的联系框架，采取有效措施，使我院管理层和各相关系部和处室的人员了解并认同我院的信息系统安全原则和管理目标。

第十二条 我院根据单位发展需要组织制定信息系统安全规划。信息系统安全规划应与本单位发展保持一致，符合本单位对信息系统安全的要求，并使技术和业务部门能正确地理解和把握我院对信息系统安全的要求。

第十三条 信息系统安全规划在有效性、可用性和安全性方面应满足我院可预见的业务发展要求，应在容量、性能和安全保障方面做出规定。

第四章 信息系统安全措施

第十四条 不得收集、研究、编制、复制、传播计算机病毒，发现计算机病毒要及时向网络与信息安全领导小组办公室报告。

第十五条 不得在计算机及网络上制作、查阅、复制、传播或执行违反国家法律法规和单位部署有关规定、危害国家和单位安全的软件或信息。

第十六条 不得在计算机及网络上制作、查阅、复制、传播或执行含有宣扬封建迷信、淫秽色情、凶杀、教唆犯罪等危害社会治安秩序内容的信息。

第十七条 不得利用电子公告服务制作、复制和传播谩骂、侮辱或诽谤单位和个人的信息。

第十八条 涉及国家或单位机密的信息，必须采取有效的保密措施，按照有关保密规定进行采集、存储、处理、传输、使用和销毁。重要信息必须从物理上进行隔离，并根据需要进行必要的数据加密。

第十九条 对计算机机房及其它重要区域须建立出入制度。

第二十条 对关键应用系统及数据的修改和备份须建立审批制度、日志管理制度、安全审计制度、系统备份制度。

第二十一条 建立帐户、密码的管理制度，严格管理操作系统、重要信息应用系统的用户口令和访问权限，建立和健全系统访问日志，保证信息共享的安全性。

第二十二条 在网络上开展电子公告服务的单位，必须对用户实行帐户管理和建立相应的信息管理制度。申请帐户需填写注册单，提供真实姓名和工作单位等资料，经一定的核实程序，方能成为电子公告服务的合法用户。

第二十三条 对服务器系统软件和个人计算机操作系统须及时进行版本升级或安装补丁程序，杜绝系统级的安全漏洞。

第二十四条 建立计算机网络病毒防治系统和计算机病毒预防、发现、报告及清除管理制度。

第二十五条 我院内部业务、财务等专用网络和单位局域网之间实现数据交换应采用适当的安全隔离措施，局域网与外单位（银行、电信和政府等部门）系统实现数据交换应采用严格的隔离措施。

第二十六条 我院局域网接入国际互联网必须经网络与信息安全工作领导小组批准方可实施，并报当地公安机关计算机安全监察部门备案。联网所采用的安全专用设备必须是经由公安部认证的产品。

第二十七条 各部门对国际互联网接入服务应记录内部用户的访问日志（包括用户、时间、访问网址和用户的网络地址）；对电子公告服务应记录发布的信息内容及其发布时间、用户及其网络地址等。

第二十八条 计算机机房应符合国家标准和其它有关规定，必须有防火、防盗、防水、防静电、防雷击、防鼠害等安全措施。在计算机机房附近施工，不得危害计算机的安全。

第五章 信息系统安全体系

第二十九条 计算机网络安全体系结构包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。充分利用各种先进的主机安全技术、身份认

证技术、访问控制技术、密码技术、防火墙技术、安全审计技术、安全管理技术、系统漏洞检测技术、黑客跟踪技术，在攻击者和受保护资源间建立多道严密的安全防线，增加恶意攻击的难度，并增加审计功能，利用这些审核信息可以跟踪入侵者。

网络安全 五层体系	安全技术、建议	应对措施
网络安全	防火墙、网络综合审计监管系统、服务器群组动态防护系统	建立完善的网络访问控制措施，安装防火墙对敏感设备和数据建立必要的武力或逻辑隔离措施； 加强主机本身的安全，对主机进行安全监管对系统资源的访问进行有效控制； 对局域网内部的服务器群组进行访问控制、入侵防御等安全措施
系统安全	入侵检测系统	检测并跟踪入侵攻击等，以便建立详细的安全审计日志； 通过检测中发现的漏洞，及时发现网络中存在的安全隐患； 对网络中的异常流量以及蠕虫病毒进行准确地定位，及时地报警，维护网络的正常运行
账号安全	互联网安全认证接入系统	对网络用户的身份进行认证，保证内部任何访问的合法性； 使用集中管理，防止因不安全密码泄漏带来的安全威胁
应用安全	网络综合审计监管系统、服务器群组动态防护系统	加强主机本身的安全，对主机进行安全监管，对系统资源的访问进行有效控制； 对局域网内部的服务器群组进行访问控制、入侵防御等安全措施
内容安全	信息审计系统	基于内容实时对网络活动进行检测，并能对非法访问及时阻断； 对于出现的非法访问，可以进行全程审计，报警，回放以及保存，为事后分析取证提供有力的保证

第六章 信息系统安全监督和处罚

第三十条 所有使用计算机的人员应积极配合我院网络与信息安全工作领导小组办公室和公安机关对计算机安全事故的查处。

第三十一条 应定期检查计算机的使用安全情况，发现有安全隐患的，应及时责成和协助使用部门或个人进行整改。

第三十二条 对计算机信息系统安全隐患严重，又不采取整改措施的，我院有权责令其停机整改。

第三十三条 对于利用电子公告服务制作、复制和传播谩骂、侮辱或诽谤单位和个人信息的，将依据单位有关规定和国家有关法律追究当事人的责任。

第三十四条 发生其它计算机信息系统安全事故的责任人或当事人将给予行政处分，情况严重的，移交公安机关惩处。

第七章 附则

第三十五条 本方案自发布之日起执行，由后勤处负责解释。

郴州技师学院个人信息管理制度

为确保学院个人信息数据规范管理、切实提高本单位个人信息保护和数据安全保障水平，学院根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等法律法规的要求，特制定本管理制度。

第一章　总则

第一条 本制度适用于郴州技师学院包括但不限于运用网络、人工等方式，开展数据采集、存储、传输、使用、处置等，与个人信息相关的所有活动。

第二条 根据相关国家法律法规和国家标准，本办法中个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于如下信息:

姓名、出生日期、身份证件号码、个人生物识别信息、银行账号、住址、个人通信通讯联系方式、通信记录和内容、账号密码、电子邮箱地址、财产信息等其他能够识别个人身份的信息。

个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，包括但不限于如下信息:

身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、健康生理信息、交

易信息、14 岁以下（含）儿童的个人信息等。

第三条 采集、存储、使用个人信息应遵循如下原则：

1.合法原则：不得违反相关法律、法规的规定；

2.最小必要原则：在满足工作开展必要需求前提下，在最小范围内采集、存储、使用个人信息，对于个人信息的处理采用最小操作权限划分，不得超范围处置个人信息；

3.安全原则：在个人信息管理工作中，应采用必要的安全技术措施和管理手段，保障个人信息的完整性、保密性及安全性，避免个人信息泄露、损毁和丢失；

4.知情同意原则：依法依规进行采集和使用个人信息，事先应明确告知相关个人，并由个人自愿同意后，方可进行。

第二章　职责分工

第四条 郴州技师学院网络与信息安全工作领导小组负责制定全单位个人信息管理的办法和规定，协调和处理全单位有关个人信息管理工作的重大问题。

第五条 后勤处负责全单位个人信息保护和数据安全保障的指导和检查工作；负责制定本单位个人信息管理制度、技术规范、控制措施等，并检查执行情况；负责组织对全体干部职工开展个人信息保护安全教育培训。

第六条 本单位领导、各部门主要负责人是落实个人信息管理工作的第一责任人。依照本办法、相关法律法规和规范要求，参照国家安全标准，履行个人信息保护和数据安全保障的责任和义务。

第七条 各部门负责本部门个人信息数据的管理工作，作为个人信息的管理者，有义务及时更新信息化建设中使用到的个人信息，保证信息的准确性和完整性， 并在信息化应用过程中妥善保管个人信息数据。由于个人原因造成的个人信息数据泄露、损坏、丢失，由本人承担相应责任；如对他人个人信息造成不良影响，将根据本办法的追责条款，追究相关责任人的责任。

第三章　个人信息数据采集

第八条 各部门因工作需要采集个人信息时，应严格按照《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》采集必要数据。数据采集原则应该遵循最小范围原则，对于身份证号、电话号码、家庭住址等个人敏感信息收集应该严格控制。非必要，则不采集。

第九条 各部门采集的数据必须经过各部门负责人审核，确保其真实可靠。

第十条 在信息化建设中，个人信息主管部门采集到的个人信息在存储和传输过程中必须进行加密处理，采取有效技术手段和管理措施保护存储个人信息的服务器和数据库，避免个人信息的泄露、损坏或丢失。原则上信息化建设中的个人信息均需要在本单位数据中心服务器本地存储，不得在非数据中心环境中存储。

第十一条 在信息化建设中，各部门采集的数据，必须严格按照业务系统的规范要求录入，确保数据全面和完整性，保证

数据操作过程可追溯。

第十二条 各部门采集产生的个人信息和重要数据，不得用于商业用途，未经采集数据的部门批准同意，不得与第三方共享。

第十三条 因阶段性工作采集产生的重要数据和个人信息，在相应工作结束后，相关数据原则上不能保留，按有关规定进行处理。

第十四条 为保障数据的规范性和准确性，各部门须向后勤处提供本部门建设的业务系统的设计文档、数据字典和数据接口等相关资料。

第四章　个人信息数据使用和处理

第十五条 本单位各业务系统主管部门负责其系统的直接使用，其他部门属于间接使用。直接使用部门负责数据的增加、修改、删除、导入、导出等，并需通过数据分类、备份、加密等措施加强个人信息保护和数据安全保障。其他部门不得对原始数据进行增加、修改、删除等操作。

第十六条 在信息化建设中，各信息化项目在使用个人信息时应严格遵循前款所述的合法原则、最小必要原则、安全原则和知情同意原则。

第十七条 各信息化项目应严格按照数据资源使用申请中所确定的用途使用个人信息，严禁将个人信息挪作他用。因信息化建设工作需要，可接触到个人信息的相关人员，对相关个人信息负有保密责任，严禁未经授权对外提供个人信息。

第十八条 各信息化项目中，对于个人信息的查询、修改等操作应保留不少于180天的最新操作日志，并提供审计功能，可审计对个人信息的各类操作。除个人信息的源数据系统，其他业务系统原则上禁止提供单独针对个人信息数据的批量导出功能。对个人信息的重要操作前（如批量修改、拷贝、导出等），需由相关信息系统主管部门负责人与后勤处负责人共同审批，审批通过后方可进行操作。

第十九条 各信息化项目应对必须要通过界面（如显示屏幕、纸面）展示的个人信息进行去标识化处理。个人信息去标识化的具体方法，请参考附件的个人信息去标识化参考指南处理。

第二十条 对于个人信息查询，原则上只接受公安、网信等网络安全主管部门依法依规的查询请求，查询请求受理部门为相关个人信息数据主管部门，其他部门和个人不得接受查询请求，严禁未经审核，私自提供个人信息数据。

第二十一条 本单位其他非个人信息管理系统需使用个人信息时需充分评估合法性、必要性和安全性，只有缺乏相关个人信息就无法正常使用的系统，在安全性可以满足个人信息保护要求的前提下，可依法依规进行个人信息共享。非数据源的各业务系统原则上不得共享个人敏感信息。

第二十二条 同一部门、同一信息系统内部由系统管理员对用户按职能分组，设定用户的访问权限，严禁跨岗位越权操作；严防非法用户或非授权用户对非授权服务、数据及文件的

访问、使用和修改等。

第二十三条 如需跨部门共享个人信息数据，需由各部门负责人、分管领导签字审核确认，方可进行共享。

第二十四条 任何部门或个人，禁止通过公共邮箱、钉钉、微信和 QQ 等公共即时通讯工具传递涉密重要数据。重要数据不得通过公共互联网传递。

第二十五条 各部门在变更应用系统数据结构时，须提前告知后勤处批准同意后才可进行变更，避免数据混乱及服务异常。

第二十六条 在信息化建设中，只有相关法律法规有明确规定需要公示的个人信息，才可进行公开。公开个人信息遵循最小化原则，通过信息组合能识别特定自然人身份并满足公示要求即可，严禁超范围公开其他相关信息，相关个人信息需进行去标识化处理，不得直接公开完整的个人信息。对于以下个人敏感信息不宜公开，包括：银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、健康生理信息、交易信息以及 14 岁以下（含）儿童的个人信息。

第二十七条 注销的信息化项目或报废的存储设备，要确保承载的个人信息已被清理才可进行注销或报废处理。对于违反法律法规及本办法采集、存储的个人信息，应依法依规删除相关个人信息数据。

第五章　个人信息数据安全

第二十八条 数据安全是指数据处理系统的硬件、软件及数

据本身受到保护，不受偶然的或恶意的原因而遭到破坏、更改和泄露。

第二十九条 坚持“涉密计算机不上互联网，非涉密计算机不处理涉密信息”的原则。涉及机密的信息系统服务器，不得直接或间接地与国际互联网或其它公共信息网络相连接，需要与业务内网相连接的服务器必须划分在专属网段进行逻辑隔离。

第三十条 为保障数据安全，各部门的应用系统须经后勤处检测合格后方可上线运行。

第三十一条 各部门需对主管的业务系统开展网络安全等级保护测评和备案工作，在发生新增、变更、撤销时要及时对备案信息进行更新。

第三十二条 各部门指定一名信息系统管理员，负责本部门业务系统管理工作，需定期进行数据安全检查，并做好检查记录。不符合相关安全保障要求的部门，必须按要求进行整改。

第三十三条 各部门自建的业务信息系统须及时打补丁和封堵漏洞，数据必须定期进行备份，并明确落实备份数据的管理职责。

第三十四条 各信息系统的管理部门需要定期对电脑、服务器、存储介质进行病毒检查，一旦发现病毒及时清除。

第三十五条 非本单位技术人员对本单位的设备、系统等进行维修、维护时，必须由本单位相关技术人员现场全程监督并做好人员登记。

第三十六条 各部门对于不再使用或无法使用的涉密信息存储介质进行报废处理时，应进行信息清除或载体销毁处理，所采用的技术、设备和措施应符合国家保密工作部门的有关规定。

第三十七条 各业务系统的管理部门不但对产生的数据负有安全管理责任，而且对参与应用系统开发建设的企业负有安全管理和约束的责任，须与其签订数据安全保密协议。

第三十八条 各部门一旦发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显增加时，应按照《郴州技师学院网络安全事件应急预案》的要求及时报告信息安全领导小组，视情况报送公安、网信网络安全主管部门，并妥善处置，将影响降到最低。

第三十九条 在履行职责中，发现相关个人信息保护和数据安全管理责任落实不到位时，应及时按照相关规定要求和程序督促整改。

第六章　责任认定及追责

第四十条 后勤处将依照本办法对各信息化项目中个人信息处置相关的审计记录进行检查，或者通过其他网络安全检测手段检查个人信息的采集、存储、使用及处理情况。对于出现的违规行为，将按照网络安全事件进行处置，相关部门及个人应按照本办法及相关整改通知，及时彻底的整改相关问题。

第四十一条 对造成重大损失或整改不力的违规行为，由后勤处负责汇总相关情况，提请郴州技师学院网络与信息安全工

作领导小组进行责任认定，确定相关责任人、责任部门，按照网络安全管理办法等相关管理制度进行追责。对于违反国家法律法规的行为，将配合公安、网信等网络安全主管部门，依法依规进行处理。

第七章　附则

第四十二条 本管理办法自颁布之日起施行、由后勤处负责解释。

附件：个人信息去标识化参考指南

附件

个人信息去标识化参考指南

在日常工作中，如需对个人信息进行去标识化处理，应保证处理后的信息无法或很难进行复原，部分信息去标识化可参考以下方法进行:

1.姓名可隐藏名字中的1-2位;

2.出生日期可隐藏2位日期;

3.身份证件号码可隐藏结尾6位;

4.个人手机号可隐藏结尾后4位;

5.个人通信地址及家庭住址可隐藏具体门牌号;

6.车牌号可隐藏后五位中的任意2-3位。

上述未说明的个人信息应遵循不可复原原则进行去标识化处理。

郴州技师学院网络安全事件应急预案

一、总则

1.1 目的

为提高学院处理突发信息网络事件的能力，形成科学、有效、反应迅速的应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公共利益，维护国家安全、公共安全、校园安全。

1.2 适用范围

本预案适用于学院内发生网络安全事件的应对工作。

1.3 工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持“谁主管谁负责、谁运行谁负责”，充分发挥各方面力量，共同做好网络安全事件的预防和处置工作。

1.4 编制依据

根据《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《计算机病毒防治管理办法》、《国家突发公共事件总体应急预案》、《突发事件应急预案管理办法》和郴州市网络安全事件应急预案管理相关规定等。

二、组织机构及职责

2.1 组织机构

学院网络与信息安全工作领导小组负责学院网络安全事件

应急处置工作。

组　　长：胡　强

第一副组长：肖武云

副 组 长：王国昌、彭德洪、邓鲜鲜、沈宏绩（常务）
刘先飞、曹　洁、李世成

成　　员：王光金、胡　晖、王建安、段志坚、
唐志雄、黎　忠、崔　励、张　理、
罗　雄、段盛琦、罗海燕、唐　燕、
陈　军、张朝气、唐玉雄、周界名、
肖雄英、陆　卫、王　军、尹锦东、
周素萍

2.2 学院网络与信息安全工作领导小组职责

学院网络与信息安全工作领导小组负责全院信息安全工作；组织制定学院信息安全应急预案及其修订、完善工作；组织协调学院网络信息安全工作中可能出现的各种突发事件的处置工作；研究解决突发事件处置工作的重大问题；对突发事件相关信息进行及时收集、分析和研判。

三、预防及预警机制

突发网络安全事件安全预防措施包括分析安全风险，准备应急处置措施，建立网络和信息系统的监测体系，控制有害信息的传播，预先制定信息安全重大事件的通报机制。

3.1 突发网络安全事件分类

特别重大网络安全事件（Ⅰ级）：重要信息安全系统发生

全院性大规模瘫痪或由于网站非法信息、谣言引发学院大规模群体性事件，对教学教研、办公秩序造成特别严重的影响，事态超出学院控制能力的突发事件。

重大网络安全事件（II 级）：重要信息安全系统发生全院性大规模瘫痪或由于网站非法信息、谣言引发师生反应强烈并有过激行为，对教学教研、办公秩序造成严重的影响，需要跨部门协调处置的突发事件。

较大网络安全事件（III 级）：学院某一区域重要网络和信息系统瘫痪或由于网站不良信息、谣言等，对教学教研、办公秩序造成一定影响，但不需要跨部门协同处置的突发事件。

一般网络安全事件（VI 级）：学院重要网络和信息系统受到一定程度的损坏，学院工作受到一定影响，但不危害正常工作秩序的突发事件。

3.2 应急准备

后勤处和各部门信息系统管理员明确职责和管理范围，根据实际情况，安排应急值班，确保到岗到人，联络畅通，处理及时准确。

3.3 具体措施

（1）建立安全、可靠、稳定运行的机房环境，防火、防盗、防雷电、防水、防静电、防尘；建立备份电源系统；加强所有人员防火、防盗等基本技能培训。

（2）实行实时监视和监测，采用认证方式避免非法接入和虚假路由信息。

（3）重要系统采用可靠、稳定硬件，落实数据备份机制，遵守安全操作规范；安装有效的防病毒软件，及时更新升级扫描引擎；加强对局域网内所有用户和信息系统管理员的安全技术培训。

（4）安装反入侵检测系统，监测恶意攻击、病毒等非法侵入技术的发展，控制有害信息经过网络的传播，建立网关控制、内容过滤等控制手段。

四、有关应急预案

4.1 机房漏水应急预案

（1）发生机房漏水时，第一目击者应立即通知后勤处，并及时报告学院网络与信息安全工作领导小组。

（2）若空调系统出现渗漏水，后勤处应立即安排停用故障空调,清除机房积水，并及时联系设备供应方处理，同时启动备用空调，必要情况下可临时用电扇对服务器进行降温。

（3）若为墙体或窗户渗漏水，后勤处应立即采取有效措施确保机房安全，同时安排通知后勤处，及时清除积水，维修墙体或窗户，消除渗漏水隐患。

4.2 网络机房长时间停电应急预案

（1）接到长时间停电通知后，学院网络与信息安全工作领导小组应及时通过 OA 系统、电话等发布相关信息，部署应对具体措施，要求停电前停止业务、保存数据。

（2）停电时间过长的，后勤处应及时报告网络与信息安全工作领导小组，及时启动备用发电设备,保证后勤处正常运转。

如有必要，网络信息与安全工作领导小组及时上报相关业务部门。

4.3 通信网络故障应急预案

（1）发生通信线路中断、路由故障、流量异常、域名系统故障后，操作员应及时通知本单位信息系统管理员，经初步判断后及时上报学院网络与信息安全工作领导小组和后勤处。

（2）后勤处接报告后，应及时查清通信网络故障位置，隔离故障区域，并将事态及时报告学院网络与信息安全工作领导小组，通知相关通信网络运营商查清原因；同时及时组织相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

（3）事态或后果严重的，学院网络与信息安全工作领导小组应及时报告上级相关业务部门。

（4）应急处置结束后，后勤处和事发部门应将故障分析报告，在调查结束后一日内书面报告学院网络与信息安全工作领导小组。

4.4 不良信息和网络病毒事件应急预案

（1）发现不良信息或网络病毒时，信息系统管理员应立即断开网线，终止不良信息或网络病毒传播，并报告学院网络与信息安全工作领导小组和后勤处。

（2）后勤处应根据学院网络与信息安全工作领导小组指令，采取隔离网络等措施，及时杀毒或清除不良信息，并追查不良信息来源。

（3）事态或后果严重的，学院网络与信息安全工作领导小组应及时报告上级相关业务部门。

（4）处置结束后，后勤处和事发部门应将事发经过、造成影响、处置结果在调查工作结束后一日内书面报告学院网络与信息安全工作领导小组。

4.5 服务器故障应急预案

（1）发生服务器故障后，后勤处应立即启动本地备份服务器，由备份服务器接管业务应用，并及时报告学院网络与信息安全工作领导小组；同时安排相关人员将故障服务器脱离网络，保存系统状态不变，取出系统镜像备份磁盘，保持原始数据。

（2）后勤处应根据学院网络与信息安全工作领导小组指令，在确认安全的情况下，重新启动故障服务器系统；重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商和上级单位，请求技术支援，作好技术处理。

（3）事态或后果严重的，及时报告学院应急领导小组。如有必要，及时上报上级相关业务部门。

（4）处置结束后，后勤处应将事发经过、处置结果等在调查工作结束后一日内报告学院网络与信息安全工作领导小组。

4.6 黑客攻击事件应急预案

（1）当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发

现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告学院网络与信息安全工作领导小组。

（2）接报告后，学院网络与信息安全工作领导小组应立即指令后勤处核实情况，关闭服务器或系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

（3）后勤处应及时清理系统，恢复数据、程序，恢复系统和网络正常；情况严重的，应上报网络信息与安全工作领导小组，并请求支援。必要时，及时上报上级相关业务部门。

（4）处置结束后，后勤处应将事发经过、处置结果等在调查工作结束后一日内报告学院网络与信息安全工作领导小组。

4.7 核心设备硬件故障应急预案

（1）发生核心设备硬件故障后，后勤处应及时报告学院网络与信息安全工作领导小组，并组织查找、确定故障设备及故障原因，进行先期处置。

（2）若故障设备在短时间内无法修复，后勤处应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（3）后勤处应在故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关建设方或厂商，认真填写设备故障报告单备查。

（4）事态或后果严重的，及时报告网络信息与安全工作领导小组。如有必要，及时上报上级相关业务部门。

4.8 业务数据损坏应急预案

（1）发生业务数据损坏时，后勤处应及时报告学院网络与信息安全工作领导小组，检查、备份业务系统当前数据。

（2）后勤处负责调用备份服务器备份数据，若备份数据损坏，立即联系相关建设方或厂商技术解决。

（3）业务数据损坏事件超过 2 小时后，后勤处应及时报告学院网络与信息安全工作领导小组，及时通知业务部门以手工方式开展业务。

（4）后勤处应待业务数据系统恢复后，检查历史数据和当前数据的差别，由相关系统业务员补录数据；重新备份数据，并写出故障分析报告，在调查工作结束后一日内报告学院网络与信息安全工作领导小组。

4.9 雷击事故应急预案

（1）遇雷暴天气或接上级部门雷暴气象预警，后勤处应及时报告学院网络与信息安全工作领导小组，经请示同意后关闭所有服务器，切断电源，暂停内部计算机网络工作，并及时通知后勤处及相关部门关闭一切网络设备及计算机等，并切断电源。

（2）雷暴天气结束后，后勤处报经学院网络与信息安全工作领导小组同意，及时开通服务器，恢复内部计算机网络工作，并通知后勤处、后勤处及时恢复设备正常工作，对设备和数据进行检查。出现故障的，事发部门应将故障情况及时报告后勤处。

（3）因雷击造成损失的，后勤处应汇同财务处等相关部门进行核实、报损，并在调查工作结束后一日内书面报告学院网络与信息安全工作领导小组。

五、网络安全事件应急处置

各部门发现网络安全事件，分析确认判定级别。第一时间向网络信息与安全工作领导小组报告。

I 级（特别重大）事件:需逐级向组长报告，并报市相关部门;

II 级（重大）事件：需逐级报至组长;

III 级（较大）事件：需逐级报至常务副组长;

VI 级（一般）事件：需向网络信息与安全工作领导小组办公室报告。

发生特别重大、重大事故（事件），无法迅速消除或恢复系统，影响较大时实施紧急关闭，并立即向网络信息与安全工作领导小组组长报告，并及时上报上级相关业务部门。

六、善后处置

应急处置工作结束后，学院网络与信息安全工作领导小组组织有关人员和技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，根据应急处置中暴露出的管理、协调和技术问题，改进和完善预案，实施针对性演练，总结经验教训，整改存在隐患，组织恢复正常工作秩序。

七、应急保障

7.1 通信保障

后勤处负责收集、建立突发网络安全事件应急处置工作小组内部及其他相关部门的应急联络信息。学院网络与信息安全工作领导小组应在重要部位醒目位置公布报警电话，学院网络与信息安全工作领导小组全体人员保证全天 24 小时通讯畅通。

7.2 装备保障

后勤处负责建立并保持电力、空调、机房等网络安全运行基本环境，预留一定数量的网络安全硬件和软件设备，指定专人保管和维护。

7.3 数据保障

重要信息系统均建立备份系统，保证重要数据在受到破坏后可紧急恢复。

7.4 队伍保障

建立符合要求的信息安全保障技术支持力量，对网络接入单位的信息安全保障工作人员提供技术支持和培训服务，选拔网络安全人员，组建网络安全支撑队伍。

八、监督管理

8.1 宣传教育和培训

将突发网络安全事件的应急管理、工作流程等列为培训内容，增强应急处置能力。加强对突发网络安全事件的技术准备培训，提高技术人员的防范意识及技能。学院网络与信息安全工作领导小组每年至少开展一次全院网络安全安全教育，提高

信息安全防范意识和能力。

8.2 预案演练

学院网络与信息安全工作领导小组每年至少安排一次演练，建立应急预案定期演练制度。通过演练，发现和解决应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

8.3 责任与奖惩

学院网络与信息安全工作领导小组不定期组织对各项制度、计划、方案、人员及物资等进行检查，对在突发网络安全事件应急处置中做出突出贡献的集体和个人，提出表彰奖励建议；对玩忽职守，造成不良影响或严重后果的，依法依规提出处理意见，追究其责任。

九、附则

9.1 预案更新

结合网络安全快速发展和学院网络建设发展状况，配合相关法律法规的制定、修改和完善，适时修订本预案。

9.2 预案实施

本预案自印发之日起实施、由后勤处负责解释。

郴州技师学院党政办公室　　2023年12月1日印发